Course ID
CYBERPOL
Course Duration
2 days

Course Title
Cyber Space and Cyber Conflict Policy

Course Type: Private Class

Related Courses

- Cyber Security and Cyber Warfare (CYBERSEC, 2 days)

Aimed At

Information/communications industry professionals, business or government security professionals, and others interested in learning how policy and regulation over the past twenty years has shaped the Internet and current legal/political issues surrounding cyber security.

Group Size

5-25

Prerequisites

General familiarity with telecommunications.

Course in a Nutshell

A spate of cyber-attacks, some of which were quite persistent and severe, have recently affected government agencies as well as businesses in a wide range of industries, including the CIA, US Senate, IMF, Google, Lockheed Martin, Sony, Citigroup, and others. This has led the Pentagon to enunciate a formal cyber strategy and Leon Panetta, the US Defense Secretary, to warn that "the next Pearl Harbor we confront could very well be a cyber-attack."

This two day course provides an overview of cyber space and cyber governance, covering both national and international policies and regulations that shape how the Internet is used and involved in cyber conflict. The course is taught by someone currently involved in pushing the state-of-the-art of cyber security/warfare technology and regulation/policy and is continually updated to include the latest research.

Customize It!

We can customize the content and duration of this course to the needs of diverse participant groups in business or government. We can also adjust the course's "tech level" to the type of your audience, such as technical professionals, managers/executives, or policy makers/strategists.

Learn How To

- Define the actors and boundaries in cyber space, and their motives and capabilities.
- Describe the legal and governance organizations associated with the Internet.
- Describe the role played by NATO, UN, and other international players.

Course Outline

- Introduction to Cyberspace
  - History of Cyberspace
    - Brief History of the Internet
    - Brief History of Internet Policy
    - Societal Reliance on the Internet and Cyber Power
    - Cyberspace as a Warfare Dimension
  - Defining Cyberspace, Control, and Borders
  - Cyber Actors: Governments, Quasi-governments, Private Entities, Intermediaries
  - Cybercrime and Cybersecurity
    - Discussion of the Threats
    - Defining the Risks
- Internet Governance
  - History: ARPANET/NSFNET and the Internet
  - ICANN
  - IETF and Standards
- United States Legal Aspects
  - Civil Law
    - Civil Liberties and Privacy
  - Criminal Law
    - Law Enforcement
  - Governmental Authorities: Law Enforcement, Intelligence, and Military
  - Case Study: Coreflood Botnet
- NATO Aspects
  - NATO Cyber Policies
  - Offensive vs. Defensive
  - Case Study: Estonia's Role in NATO Cyber Policy
- United Nations Aspects
  - Proposed Cyber Security Treaty
  - China and Russia's Role
  - Cyber as a Human Right
- Case Study: Wikileaks and Anonymous
- Industry Collaboration and Public/Private Partnerships
  - Opportunities for International Collaboration, such as APEC
  - FIRST, CERT
  - Industry Groups
- Wrap-up
  - Course Recap and Q/A
  - Evaluations

How You Will Learn

- A researcher who is at the forefront of cyber security/warfare and policy/regulation will present this course in interactive lecture format.
- Along with the lecture, we will use discussion and group activities to enrich the classroom environment and convey the important points.
- We will compare and contrast what's already familiar to you with what's new, making the new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use meaningful and ingenious examples and analogies to simplify the complex subject matter.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

Revised *July 21, 2011f*